PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/20 — A1

(11) International Publication Number: **WO 98/28929**

(43) International Publication Date: 2 July 1998 (02.07.98)

(21) International Application Number: PCT/FI97/00746

(22) International Filing Date: 2 December 1997 (02.12.97)

(30) Priority Data:
964876 5 December 1996 (05.12.96) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HOKKANEN, Petri [FI/FI]; Koivumutka 21, FIN–40270 Palokka (FI).

(74) Agent: PATENT AGENCY COMPATENT LTD.; Teollisuuskatu 33, P.O. Box 156, FIN–00511 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

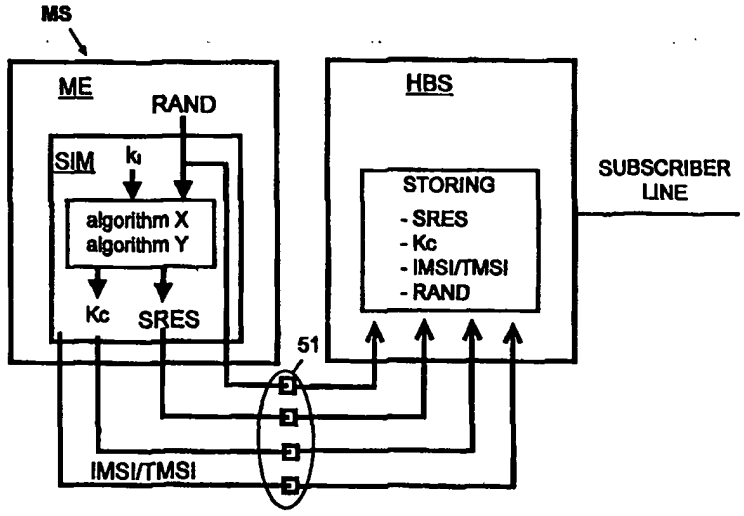
Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

In English translation (filed in Finnish).

(54) Title: USE OF A MOBILE STATION AS A CORDLESS TELEPHONE



(57) Abstract

Turning of a cellular network phone (MS) into a cordless phone begins by placing the phone in a charging device located in a home base station (HBS) and containing special communication pins through which the phone and the base station may exchange authentication information while the phone is in the charger. When there is a wireline connection between the home base station and the phone, any party may generate the authentication and ciphering information provided that the information is agreed upon in advance. According to a preferable embodiment, the parameters (RAND, SRES, Kc) used for authentication are generated by the mobile station and the parameters are transmitted through a fixed connection to the home base station which stores them. When the phone is removed from the home base station and a call is formed, the base station sends an inquiry (RAND) to which the mobile station gives a response (SRES) and if the home station finds that the response and a value earlier stored in memory are identical, a subscriber connection will be formed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

USE OF A MOBILE STATION AS A CORDLESS TELEPHONE

Field of the invention

This invention concerns a cellular system comprising base stations and mobile stations with an interface in between which is a radio interface.

Background of the invention

In a fixed wireline network the calling subscriber knows the grounds for charging of the call even when dialling the number of subscriber B, because debiting will depend on whether the call is a local call, a long distance call, a mobile call or a call to a foreign country. The terminal equipment used by subscriber A also affects debiting, since mobile originated calls are more expensive than calls originated from a fixed network, irrespectively of the target terminal equipment. This can be seen as the price which the subscriber will have to pay for his great freedom of movement.

The ordinary home user has long been offered cordless phones providing a limited mobility. The arrangement comprises a base station at the subscriber line end which converts the audio signal arriving from the fixed network into a radio signal and transmits it further to the cordless phone. The most usual modulation used so far is FM modulation. The major drawback of this kind of modulation is that traffic in the radio path be listened to illegally by any FM receiver tuned to a suitable frequency. An essential improvement on this is to use digital modulation and transfer of speech ciphered over the radio path. A suitable and already standardized digital system is the DECT system (Digital European Cordless Telecommunications), and cordless phones complying with the specification of this system and intended for home users are in fact already available.

A great disadvantage of the cordless phone is the limitation of the allowed mobility to a radius of 50-100 m from the base station , but an advantage is the cheaper prices of the fixed network compared with e.g. the mobile network. Another great disadvantage is low security especially when using the traditional analog system.

The grounds for charging of the call used in a fixed network may not be used as such in mobile networks allowing great mobility due to the network structure and manner of operation. In the following the structure and operation of the mobile network will be explained using the known GSM

mobile network shown in Figure 1 as an example. Communication between the MS (Mobile Station) in a cell and the network takes place through the radio via the base station BTS (Base Transceiver Station). Base stations BTS are connected to the BSC (Base Station Controller), with e.g. radio channel management and channel exchange functions as its duties. Several base station controllers are connected to one MSC (Mobile Switching Center) performing the major switching functions of the mobile network and connecting the mobile network with other mobile switching centers and with external networks.

The mobile network also comprises various databases, such as an HLR (Home Location Register), where subscriber information is stored permanently. The subscriber's MSISDN number, the IMSI (International Mobile Subscriber Identity) used within the network and subscriber service information are stored in the home location register as well as routing information to the VLR (Visitor Location Register). The AuC (Authentication Center) is also located in connection with the home location register. Subscriber information received from HLR is stored in VLR for the time it takes for the visitor to stay in the VLR area.

When doing location updating for the first time, the network will check whether the user has right to access to the network. The purpose of the security functions of the GSM system is to prevent unauthorized access to the network, thus preventing anyone from using the network for somebody else's account and to protect the user's privacy. Unauthorized access is prevented through authentication, where the user is identified to make sure that the subscriber is entitled to use the network. In fact, the MS is formed of two parts: the ME (Mobile Equipment) and the SIMcard (Subscriber Identity Module), so an operating mobile station MS is formed only by pushing the SIM card into the mobile equipment ME. The identification by having the user push his SIM card into his mobile station MS is intended to prevent unauthorized use of e.g. stolen equipment and to make sure that only those subscribers use the network who pay their bills. From the operator's point of view, identification is especially important particularly in connection with international roaming, since the network does not know the visitor's subscriber information and is thus unaware of any insolvency.

Firstly, the user identifier or PIN code (Personal Identity Number) given by the user himself and stored on the SIM card is used in identification.

In the first stage, when electric power is turned on to the phone, the phone will ask the user to push a code of 4-8 digits and will compare the entered code with a code stored in the memory. If the code is incorrect after three attempts, the card will go into a locked state and it can not be opened without special measures. This identification is done entirely locally by the SIM card, so no PIN code is transmitted by radio and the code can thus not be captured.

Secondly, after the correct PIN code has been entered, the mobile station will transmit its IMSI number to the network or, if possible, a TMSI (Temporary Mobile Subscriber Identity), whereupon authentication between network and card will take place, which will be explained by referring to Figures 1 and 2.

The principle is such that the network will put a question to the mobile station to which only the right SIM card will know the answer. In the fixed part of the network, identification is performed by the AuC (Authentication Center) located in connection with the home location register HLR while the SIM card performs identification in the terminal equipment. Identification is based on identification algorithm A3 and on subscriber-based identification key K_i. The IMSI (International Mobile Subscriber Identity), the subscriber-specific key K_i and the identification algorithm A3 mentioned above are stored both in the network and in the SIM card.

Figures 1 and 2 are referred to in the following. In the early part of identification, the authentication center AuC will send a question to the mobile station, which is a random number RAND having a length of 128 bits. Thus, its value is in a range of 2^{128}-1, so there is a very small chance that the same random number could be used twice. This stage is represented in Figure 1 by circled figure one and in Figure 2 by an arrow passing through the radio interface. The mobile station receives RAND, transfers it to the SIM card, which performs the A3 algorithm with its aid and with the aid of the subscriber-specific key K_i located in the card. The resulting answer is a 32-bit SRES (Signed Response) which the mobile station sends to the network. Authentication center AuC receives it, the circled figure two in Figure 1, and compares the SRES value with the value which it has calculated itself using the same A3 algorithm as well as RAND and key K_i. If the SRESs are the same, the identification is accepted, otherwise the subscriber will not be permitted access to the network (the yes/no stage in Figure 2).

Figure 3 illustrates how the mobile station uses received RAND and K_i values also for the A8 algorithm, which produces a connection-specific ciphering key Kc, which is used further as a key for a third algorithm A5, which is used for ciphering speech and data on radio traffic channels. In the network the AuC performs the same algorithm with the same values and thus obtains the same ciphering key as result. Both store the key in memory.

Since the identification information is always calculated in the home network, operators may use different A3 and A8 algorithms and they will not know what algorithms the other uses. On the other hand, the speech ciphering algorithm A5 must be the same in all networks.

Thus, of all the information contained in the SIM card, the IMSI, K_i and algorithms A3 and A8 are important to identification. Algorithms A3 and A8 are performed in the SIM card so that key K_i need never be transmitted between the card and the mobile equipment ME proper.

As was said above, calculation of the identification data always takes place in the AuC of the subscriber's home network. This being the case, when the subscriber is in another network identification would immoderately load the signal network between VLR and AuC. To avoid this, AuC generally sends ready triplets to the visitor location register VLR while the visitor is registering into this. The triplet contains the RAND, SRES and Kc. Hereby, the visitor location register will check whether the mobile station has calculated correct values, so that signalling to the AuC may be reduced.

It is realized from the above presentation that in terms of security the digital cellular system is very advanced as regards unauthorized use and speech ciphering. Since all cells are of equal value for the mobile network, no other grounds for calculation of the price of calls can be offered than e.g. flexing based on the hours of the day and night and cheaper than normal prices between mobile station and home phone. No special charging grounds can be offered for a call originated from or terminated in a certain cell. These factors reduce the use of the mobile phone as a home phone.

It has been suggested in the field to arrange at home or in any other place desired by the subscriber a special HBS (Home Base Station) which can be connected to an ordinary telephone connection and which is as simple a device as possible serving only one or just a few users registered with the base station, who use a normal phone in a cellular network. As regards its functions the home base station would thus correspond to present

base stations for cordless phones, that is, it performs a conversion between the wireline network and the radio interface. Even if the base station would be in the nature of a "stripped" base station in a cellular network, it would be necessary in one way or another to authenticate a cellular network phone desiring access to the network through the base station. The phone does in fact always work in the same manner in authentication and expects to receive a RAND inquiry from the network. At least two ways have been proposed.

Firstly, a modem connection could be arranged from the home base station to the authentication center AuC of the cellular network, whereby parameters to be exchanged in authentication are transferred through this connection and authentication proper would take place in a normal manner as shown in Figure 2. Since signalling would pass through another network than the network of the cellular network operator, an agreement on the matter must be made with the operator in question.

Secondly, a card reader could be located in the home base station and a special card could be used containing data relating to this base station and user. Hereby authentication would be performed between card and base station, so the user would activate the base station with his card.

Drawbacks of these proposed procedures are difficult modem signalling over a fixed network (e.g. PSTN) and acquisition of extra cards and readers as well as the making of related software.

The present invention thus aims at bringing about a cordless telephone system which is based on a cellular network and which does not have the presented drawbacks and wherein standard terminal equipment of the cellular network may be used at home as cordless phones without any special steps required of the user, which thus allows cheaper calls.

The objectives are achieved with the attributes presented in the independent claims.

Brief summary of the invention

The proposed home base station which is connected to an ordinary telephone connection contains in the manner of a base station for known cordless phones a charging device where the phone can be charged. Besides the pins supplying the charging current, it has special communication pins through which the phone and the base station can exchange

authentication information while the phone is in the charger. The turning of the cellular network phone into a cordless phone thus begins by placing the phone in the charger.

In authentication all information transfer takes place only between base station and phone while the authentication center AuC of the cellular network is entirely outside. Hereby, since there is a wireline connection between the home base station and the phone, it does not matter which party's authentication means will generate the authentication and ciphering data as long as these are agreed upon in advance. Even the algorithms need not be such which are used in the cellular system. It is enough to agree in advance that when one party sends a certain inquiry, the other party will respond with a certain answer, whereupon both will use an agreed ciphering key in the radio traffic. The authentication is invisible to the user.

According to an advantageous embodiment, the parameters used in authentication are generated by first means located in the mobile station and the parameters are transferred through a fixed connection to second means which are located in the home base station and which will store them. This makes the base station simpler. In addition, it is advantageous to use the same inquiries, responses, algorithms and ciphering keys as in the cellular system with which the phone in question complies. Hereby any software changes to be made in the phone will be minor changes.

According to another embodiment, the parameters used in authentication are generated by second means in the base station and the parameters are transferred through a fixed connection to such first means in the mobile station which will store them.

It is advantageous when placing the phone in the charger that deregistration of the phone from the cellular network will start at the same time. Hereby any transfer of a call to the home phone will work normally, should the mobile station not answer. Information from the cellular network time may be left in the phone memory, whereby it may be put into use when the phone moves over to the cellular network. Such putting into use may take place automatically, when the phone moves outside the range of the home base station.

When the mobile station has turned into a cordless phone, authentication is performed in the beginning of the call formation using parameters which have been calculated in advance and stored in the memory.

List of figures

The invention will be explained in greater detail referring to the appended schematic figures, wherein

Figure 1 shows the principle of a cellular system;
Figure 2 shows authentication in a known cellular system;
Figure 3 shows formation of a ciphering key in a known system;
Figure 4 shows the principle of a system according to the invention;
Figure 5 illustrates registration in a system according to the invention;
Figure 6 illustrates authentication in a system according to the invention;
Figure 7 depicts another embodiment; and
Figure 8 shows authentication in the other embodiment.

Detailed description of the invention

Figure 4 shows basic elements of the system. A subscriber line 1 comes to the subscriber's home, office or any other such place from the local exchange of a fixed PSTN or ISDN network 3. Subscriber line 1 is connected to a HBS (Home Base Station), which will convert speech and data arriving from the subscriber line into the format of the air interface of the cellular system and will send it further to radio communication and will correspondingly convert speech and data arriving in cellular system form from radio communication into the form used in the fixed network, in the case of a PSTN network into an audio signal and in the case of an ISDN network into a PCM signal. The transmission power is low to minimize the interference caused by frequencies used in the home base station, so the cell radius is of the same magnitude as with cordless phones, a few hundred meters in free space.

On the other hand, basic elements comprise a mobile station MS which is a device in accordance with some digital cellular system. The known GSM system is used as example.

When moving within the area of the cellular system, the mobile station is in connection with the base station providing the best connection at each time and it will traffic in a normal manner in the cellular network. When the user moves in the cellular network from place A to his home in place B, which move is shown by an arrow, the mobile station MS will still remain

registered with the cellular network. Only when the user connects his phone with a wireline connection directly to the home base station, arrow A -> C, will deregistration of the phone from the cellular network take place. The charging station for phone batteries in the home base station, represented by a depression in home base station HBS, may contain, besides charging current pins, one or more contact pins, whereby when the phone is placed in the charging station the contact pin will be brought into contact with a corresponding pin in the phone, which will start both deregistration of the phone from the cellular network and registration with the home base station.

According to a first embodiment, all calculation relating to authentication is performed in mobile station MS. This embodiment will be explained referring to Figure 5.

Registration with the home base station takes place so that the subscriber equipment ME generates a random number RAND, which it feeds to the SIM card. The SIM card calculates an algorithm X using the random number and key K_i obtaining SRES as result. Using the same values but algorithm Y the SIM card performs algorithm Y obtaining a connection-specific ciphering key Kc as result. These algorithms may be the same as those used in the cellular system, that is, in case of a GSM system algorithms A3 and A8, but they may as well be any algorithms. The SIM card will also give the IMSI (International Mobile Subscriber Identity) or the TMSI (Temporary Mobile Subscriber Identity), which may be any accepted value. In its main features the function corresponds to the left side of Figures 2 and 3, except that ME instead of the authentication center AuC will generate the random number RAND.

The SIM card will feed the response SRES which it has generated, the key Kc and the IMSI/TMSI value to subscriber equipment ME, which will transmit them along a fixed connection through contacts pins 51, which connect the mobile station and the home base station HBS, to home base station HBS, which will store the data it received. Registration has now taken place and the home base station knows the authentication and ciphering parameters which are used. The mobile station MS has turned into a cordless phone, it may be removed from the home base station HBS and it may start or receive a fixed network call. Its phone number is the number given by the fixed network operator to this subscriber connection.

When starting or receiving a call, the first step to perform is authentication, which is explained referring to Figure 6. First, the mobile station MS sends to the home base station HBS by radio its identifier TMSI, which the home base station uses to search from its memory such values received earlier from the mobile station which relate to the identifier. Thereafter the home base station will authenticate the mobile station by sending to it the RAND number which it has retrieved from the memory. Upon receiving the RAND, the SIM card will perform algorithm X, obtaining the SRES value as result, which the mobile station MS will send to the home base station. The value ought to be the same as the one it has generated earlier in connection with the registration, so the home base station will perform validation by comparing the received SRES value with the one in its memory. If they are identical, the call may be started. For ciphering the information it has sent to the mobile station the base station uses ciphering key Kc which it has stored, and the mobile station uses the same key, which it has also stored earlier, or then it may recalculate the key using algorithm Y, as shown in the figure.

It should be noticed that both the RAND and the SRES values may be sent even several times over the radio interface, whereby a third party may capture them. This is possible also in case of a GSM system. However, this is not a problem, because the ciphering key is not transmitted at all by radio, but only through the fixed connection when the mobile station is attached to the home base station.

Figure 7 shows another embodiment, where the home base station is the active party in authentication.

Registration with the home base station takes place so that the mobile station MS transmits its IMSI (International Mobile Subscriber Identity) or its TMSI (Temporary Mobile Subscriber Identity) to the home base station HBS. In response to this, the home base station will generate a random number RAND and calculate algorithm X using the random number and key K_i, obtaining the answer SRES as result. Using the same initial values but algorithm Y it also performs algorithm Y obtaining a connection-specific ciphering key Kc as result. These algorithms may be the same as those used in the cellular system. All values are stored in the memory.

Hereafter the home base station feeds its generated inquiry RAND, its calculated answer SRES and the key Kc through contact pins 51

to subscriber equipment ME, which will store the information it receives. Registration has now taken place and the authentication and ciphering parameters to be used are now known to the mobile station. The mobile station MS has turned into a cordless phone, it may be removed from home base station HBS and it may originate or receive a fixed network call.

When originating or receiving a call, authentication is first performed and this is explained referring to Figure 8. The mobile station MS first sends by radio to home base station HBS its identifier TMSI, which the home base station uses for finding from its memory any values which relate to the identifier and which have earlier been received from the mobile station. Thereafter the home base station authenticates the mobile station by sending to it the RAND number which it has searched from the memory. Having received the RAND, the SIM card will perform algorithm X obtaining as result the SRES value, which the mobile station MS will send to the home base station. The value ought to be the same as the one which it generated earlier in connection with the registration, so the home base station performs validation by comparing the SRES value which it has received and the one in its memory. If these are the same, the call may be started. For ciphering the information it has sent to the mobile station, the base station uses the ciphering key Kc which it has stored, and the mobile station uses the same key, which it too has stored earlier, or then it may recalculate the key using algorithm Y.

It is also possible to act in such a way that the mobile station authenticates the base station. Hereby it sends to the base station both the IMSI and the RAND, in response to which the base station returns the SRES number. The mobile station checks to make sure that the number corresponds with the already stored or recalculated SRES value.

Arranging functions according to the invention in present cellular network phones will require minor software additions and new algorithms, if required, in addition to the existing ones, such as A3A8 algorithms. Any additions to be made in the home base station are minor ones, if the first embodiment is implemented. The great advantage is that any cellular network phone registered with the home base station will work as a cordless phone. In practice, the phone is a dual-mode phone, whereby the same phone will work at home as a cordless phone at cheaper call tariffs and outside the home as a normal cellular network phone. If registration with the

base station takes place automatically, as proposed above, and if registration with the cellular network takes place automatically using earlier parameters stored in the phone memory, the user to change the mode need only connect the phone for a moment to the home base station when coming home, to the office or any other such place.

When the phone registers with the home base station, one must of course make sure that its transmission power will fall considerably below the minimum transmission power determined for the mobile station in the cellular network system so that the range will be reduced to a few hundred meters in free space. This must be done because when operating as a cordless phone the mobile station will not cause interference in such connections of the cellular system which use the same frequency.

It could even be possible to program the phone so that it would be able when registered with the home base station to receive calls both from the fixed network side and from the cellular network side, but outgoing calls would be directed to the fixed network.

The proposed arrangement can be implemented in practice in many different ways keeping within the scope of the claims. Programs and algorithms can be freely chosen as well as the party who will generate the authentication and ciphering information. Registration may preferably be started by pushing the phone into the charging station, but the base station may alternatively have some other place where the phone is placed while registration takes place. Several phones may be registered with the home base station. In-house calls between these phones may be implemented by suitable software in the base station.

Claims

1. Telephone system comprising terminal equipment and a home base station connected with a subscriber line to a telephone exchange, whereby a part of the subscriber connection is formed by a radio link between the terminal equipment and the base station,

characterized in that

the terminal equipment is a mobile station of a cellular mobile telephone system also containing first means for implementing an authentication procedure between itself and the home base station (HBS),

the base station contains second means for implementing an authentication procedure between itself and the mobile station,

generation and exchange of authentication parameters between the mobile station and the home base station begin at once when the mobile station is put into the home base station so that a wireline connection is brought about between them, whereby after transmission of authentication parameters the mobile station has turned into a cordless phone registered with the home base station.

2. System as defined in claim 1,

characterized in that

the first means comprise a first algorithm (algorithm X), an identification key (K_i) and a random number (RAND) generator,

the second means comprise a memory,

after putting the mobile station in the home base station the first means will generate a random number (RAND), in response to which the first algorithm (algorithm X) produces an answer (SRES) using identification key (K_i) and the mobile station transmits the random number (RAND), the response (SRES) and its identifier (IMSI/TMSI) to the home base station (HBS) to be stored in the memory.

3. System as defined in claim 2,

characterized in that

the first means comprise a second algorithm (algorithm Y) and in response to the random number the first means will perform a second algorithm (algorithm Y) using the random number and the identification key (K_i) and as result of the second algorithm transmit a connection-specific ciphering key (Kc) to the home base station to be stored in the memory.

4. System as defined in claim 1,

c h a r a c t e r i z e d in that

the first means comprise a memory,

the second means comprise a first algorithm (algorithm X), an identification key (K_i) and a random number (RAND) generator,

after putting the mobile station in the home base station, the mobile station transmits its identifier (IMSI/TMSI) to the home base station, in response to which the second means will generate a random number (RAND), in response to which the first algorithm (algorithm X) will produce a response (SRES) using identification key (K_i) and the home base station will transmit the random number (RAND) and the response (SRES) to the mobile station to be stored in the memory.

5. System as defined in claim 4,

c h a r a c t e r i z e d in that

the second means also comprise a second algorithm (algorithm Y) and in response to the random number (RAND) the second means will perform a second algorithm (algorithm Y) using the random number and the identification key (K_i) and will as result of the second algorithm transmit a connection-specific ciphering key (Kc) to the mobile station to be stored in the memory.

6. System as defined in claim 2,

c h a r a c t e r i z e d in that when the mobile station works as a cordless phone separately from the home base station, authentication information of the call is performed in such a way that

a) the mobile station sends its identifier (IMSI/TMSI) to the home base station,

b) in response to the identifier the home base station searches the memory for the stored random number (RAND) and sends it to the mobile station,

c) in response to the random number (RAND) the mobile station searches the memory for the stored response (SRES) and sends it to the home base station,

d) the home base station compares the response which it received with the response it has stored in the memory and accepts the mobile station if the responses are identical.

7. System as defined in claim 4,

characterized in that when the mobile station works as a cordless phone separately from the home base station, authentication in formation of the call is performed in such a way that

a) the mobile station sends its identifier (IMSI/TMSI) to the home base station,

b) in response to the identifier the home base station searches the memory for the stored random number (RAND) and sends it to the mobile station,

c) in response to the random number (RAND) the mobile station performs a first algorithm (algorithm X) using the random number and the identification key (K_i) and sends the resulting response (SRES) to the home base station (HBS),

d) the home base station compares the response which it received with the response it has stored in the memory and accepts the mobile station if the responses are identical.

8. System as defined in claim 6 or 7,

characterized in that the mobile station ciphers the information it sends using the connection-specific ciphering key (Kc) which it has stored in the memory, and the home base station ciphers the information it sends using the connection-specific ciphering key (Kc) which it has stored in the memory.

9. System as defined in claim 1, characterized in that when the mobile station is placed in the home base station, it deregisters automatically from the cellular network.

10. System as defined in claim 1, characterized in that when the mobile station is placed in the home base station, it deregisters automatically from the cellular network but keeps in memory the authentication parameters used in the cellular network, whereby when the mobile station moves beyond the range of the home base station it will automatically attempt access to the cellular network using these parameters.

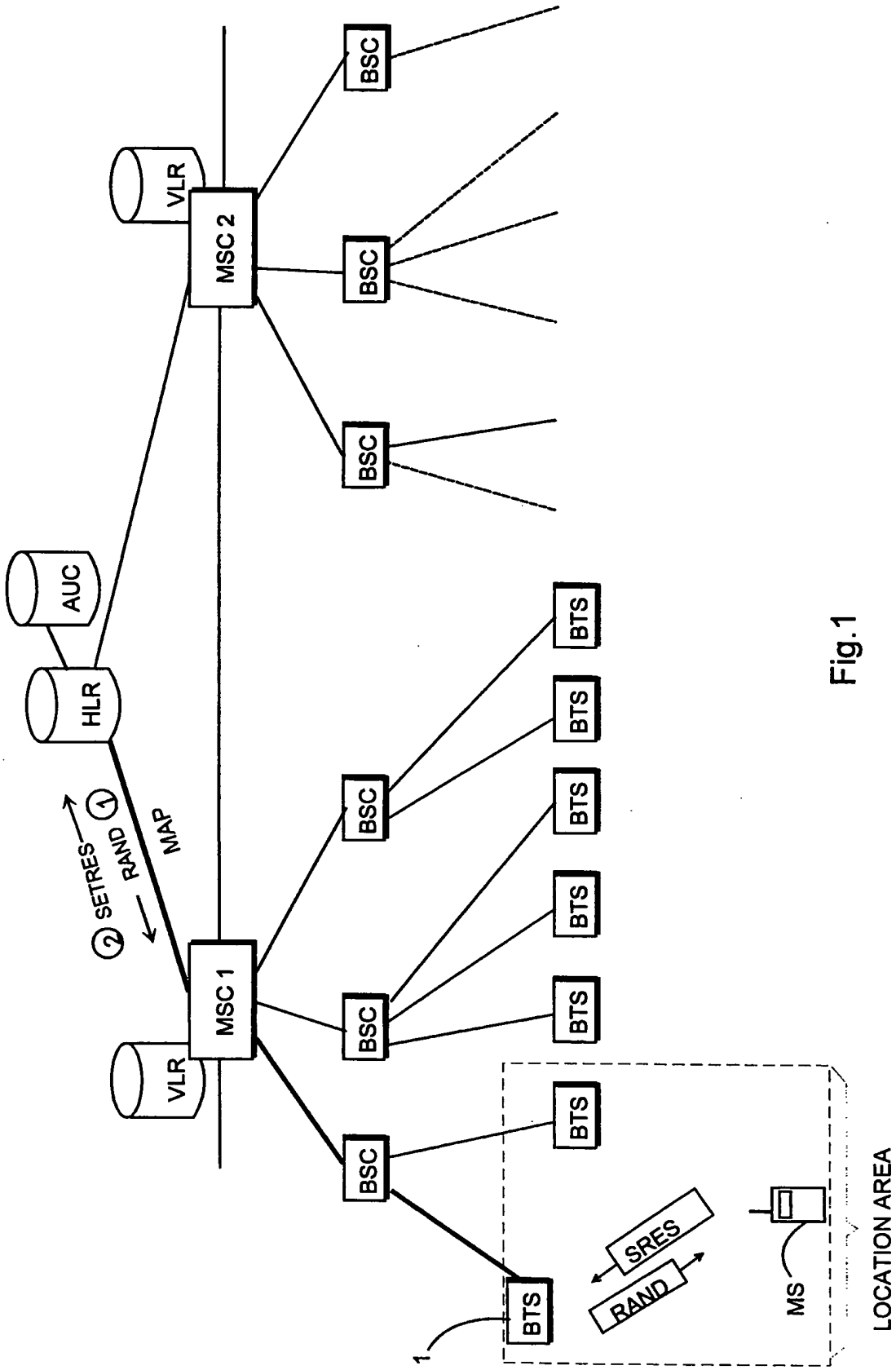

VLR
MSC 2
BSC
BSC
BSC
AUC
HLR
MAP
SETRES
RAND
MSC 1
VLR
BSC
BSC
BSC
BSC
BTS
BTS
BTS
BTS
BTS
BTS
BTS
SRES
RAND
MS
LOCATION AREA
1

Fig.1

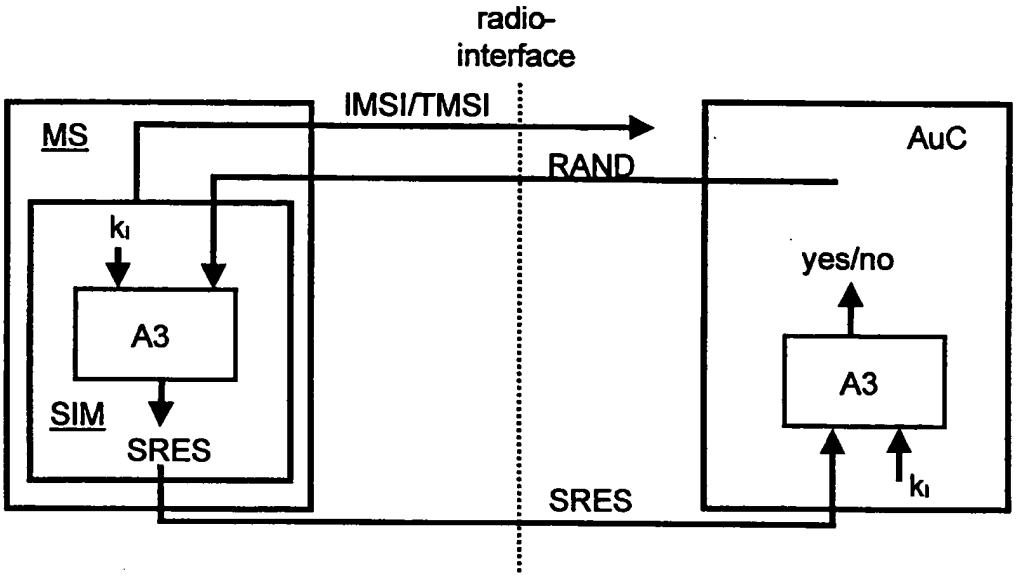

radio-
interface
IMSI/TMSI
MS
AuC
RAND
ki
yes/no
A3
A3
SIM
SRES
SRES
ki

Fig. 2

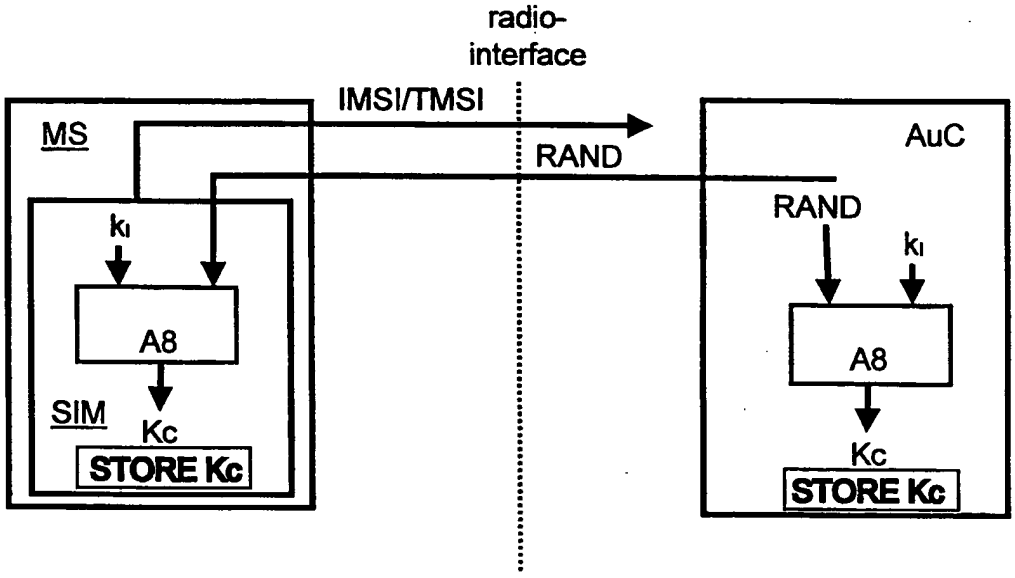

radio-
interface
IMSI/TMSI
MS
AuC
RAND
RAND
ki
ki
A8
A8
SIM
Kc
Kc
STORE Kc
STORE Kc

Fig. 3

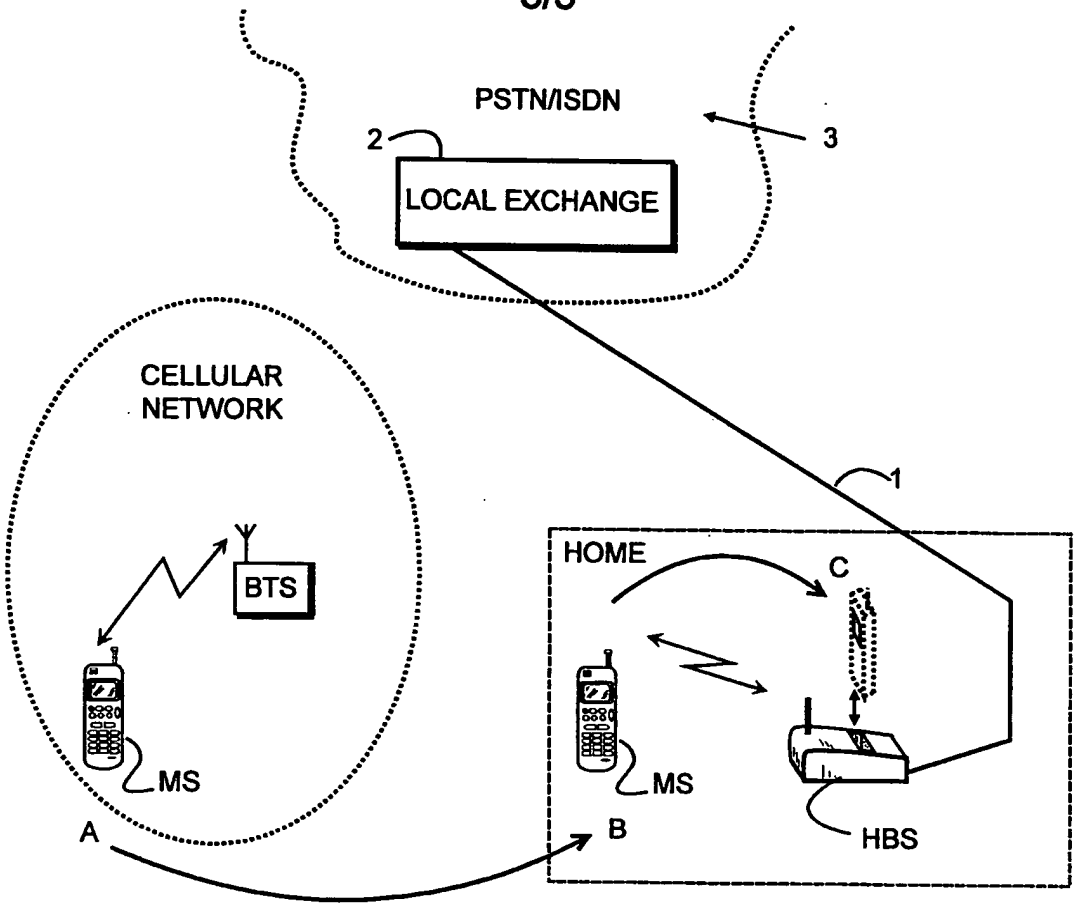

PSTN/ISDN
2
3
LOCAL EXCHANGE
CELLULAR
NETWORK
1
BTS
HOME
C
MS
MS
A
B
HBS

Fig. 4

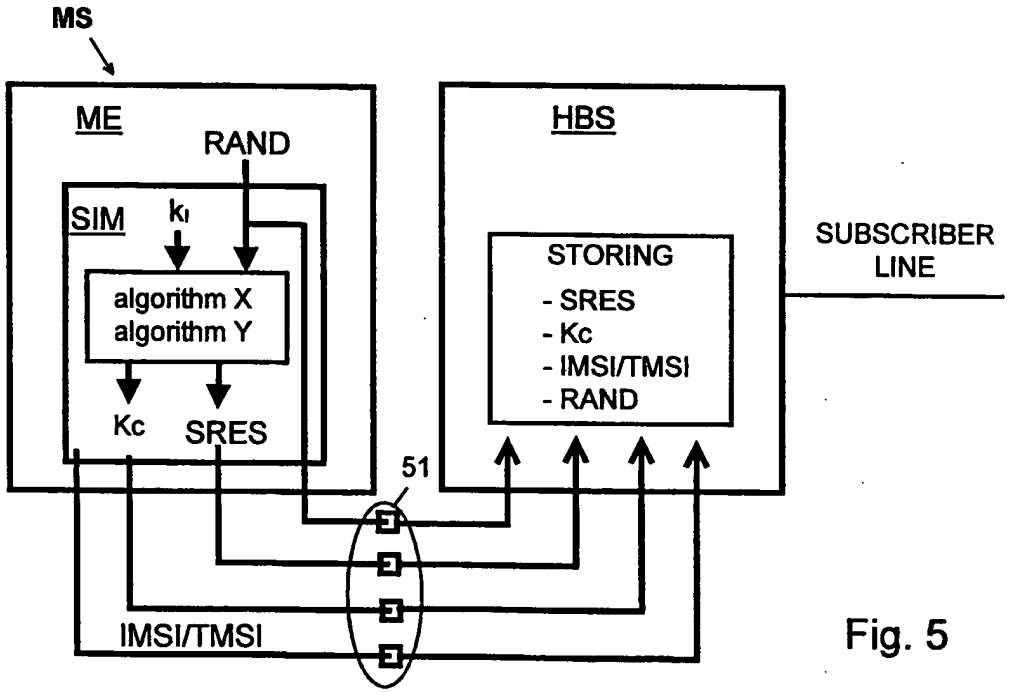

MS
ME
RAND
SIM
ki
algorithm X
algorithm Y
Kc
SRES
HBS
STORING
- SRES
- Kc
- IMSI/TMSI
- RAND
SUBSCRIBER
LINE
51
IMSI/TMSI

Fig. 5

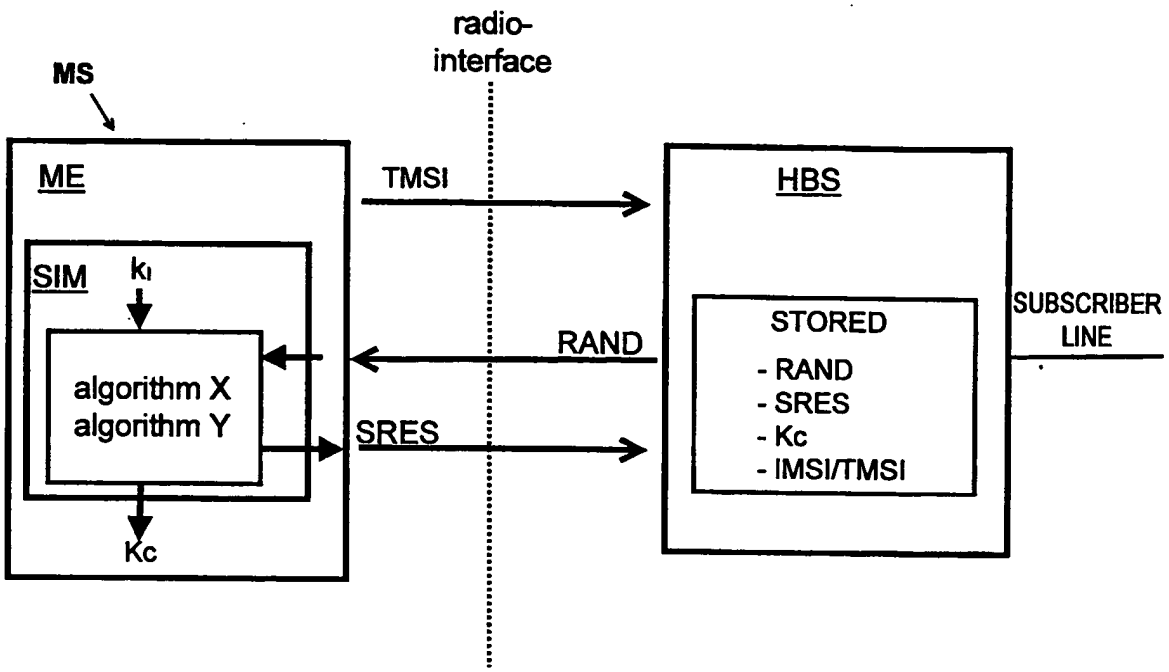

radio-
interface
MS
ME
SIM
ki
algorithm X
algorithm Y
Kc
TMSI
RAND
SRES
HBS
STORED
- RAND
- SRES
- Kc
- IMSI/TMSI
SUBSCRIBER
LINE

Fig. 6

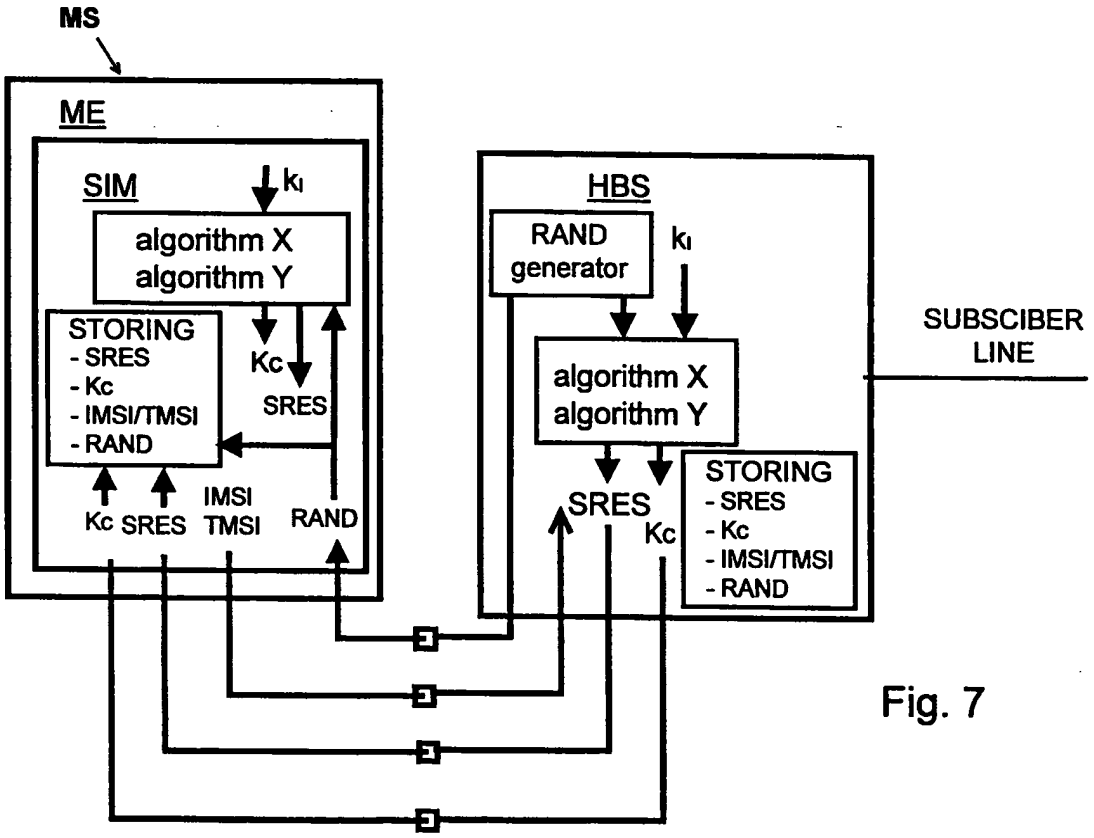

MS
ME
SIM
ki
algorithm X
algorithm Y
STORING
- SRES
- Kc
- IMSI/TMSI
- RAND
Kc
SRES
Kc SRES IMSI TMSI RAND
HBS
RAND
generator
ki
algorithm X
algorithm Y
SRES
Kc
STORING
- SRES
- Kc
- IMSI/TMSI
- RAND
SUBSCIBER
LINE

Fig. 7

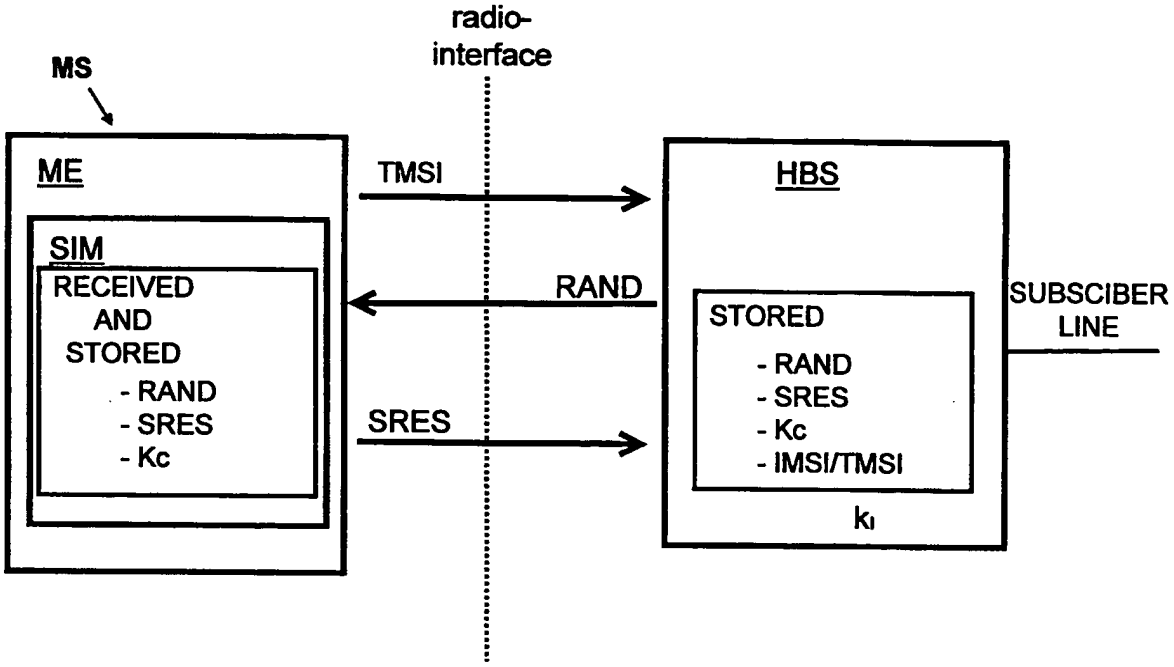

radio-
interface
MS
ME
SIM
RECEIVED
AND
STORED
- RAND
- SRES
- Kc
TMSI
RAND
SRES
HBS
STORED
- RAND
- SRES
- Kc
- IMSI/TMSI
ki
SUBSCIBER
LINE

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00746

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/20
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9524106 A1 (ERICSSON INC.), 8 Sept 1995 (08.09.95), page 4, line 16 - line 36; page 5, line 29 - line 36; page 6, line 28 - page 7, line 5, page 18, line 29 - page 19. line 20, page 20 line 29 - line 34	1-10
A	EP 0740482 A1 (HEWLETT-PACKARD COMPANY), 30 October 1996 (30.10.96), column 2, line 42 - column 3, line 4; column 3, line 15 - line 40; column 5, line 27 - line 46, abstract, column 5, line 55 - column 6, line 13. see figures	1-10

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 1998	05 -05- 1998
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Göran Petersson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 97/00746

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9501070 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 5 January 1995 (05.01.95), page 23, line 19 - line 25; page 24, line 18 - line 36; page 27, line 3 - line 31 --	1
A	GB 2225512 A (MOTOROLA INC), 30 May 1990 (30.05.90), page 7, line 1 - line 29; page 11, line 1 - line 34; page 15, line 23 - line 30 --	1
A	GB 2285556 A (MOTOROLA LIMITED), 12 July 1995 (12.07.95), page 2 - page 7 --	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/04/98

International application No.
PCT/FI 97/00746

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9524106 A1	08/09/95	AU 1922395 A	18/09/95
		CA 2183152 A	08/09/95
		CN 1142307 A	05/02/97
		EP 0748573 A	18/12/96
		FI 963420 A	02/09/96
EP 0740482 A1	30/10/96	NONE	
WO 9501070 A1	05/01/95	AU 7089294 A	17/01/95
		CA 2163745 A	05/01/95
		CN 1126017 A	03/07/96
		EP 0705522 A	10/04/96
		FI 956144 A	20/12/95
		JP 8511925 T	10/12/96
		NO 955209 A	21/02/96
		SE 9302161 A	23/12/94
GB 2225512 A	30/05/90	CA 1292041 A	12/11/91
		HK 42596 A	22/03/96
		JP 2528001 B	28/08/96
		JP 3001621 A	08/01/91
		JP 8237747 A	13/09/96
		US 4989230 A	29/01/91
		US 5127042 A	30/06/92
		US 5367558 A	22/11/94
		US 5463674 A	31/10/95
GB 2285556 A	12/07/95	NONE	